Agenda

• Is O365 Secure?

• How do we make O365 Secure for us?

• Best Practices
Is O365 Secure?

Yes, but...
Cybersecurity is Our Shared Responsibility!
The secret to doing anything is believing that you can do it. Anything that you believe you can do strong enough, you can do. Anything. As long as you believe.
What is Cyber Security?

Cyber Security is a set of principles and practices designed to safeguard your computing assets and online information against threats.

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, security includes both cybersecurity and physical security.
Balance opportunities/operations & security risks

**OPPORTUNITIES**
- Agility
- Cost
- Transformation
- Modernization

**SECURITY RISKS**
- Data loss
- Downtime
- Privacy breach
- Malware attacks

**SECURITY STRATEGY**
How do we make O365 Secure for us?

- O365 Governance
- Monthly Security meetings with CISO
- Quarterly Meetings with other States
- Service Packages
- Service Transition Readiness Assessment Checklist (STRAC)
- Yearly Service Maturity Assessment
- Agency Kickoff meetings for each service
- O365 Community of Practice (COPs) / Workgroups
- Tenant Owner Guidance
- Purchase O365 Government Skus
- Must be on a supported OS and Office Version
O365 Governance – Why?

- Need for a central body to make decisions for the State tenant(s)
- Set Baseline Security
- Provide a 2 way feedback mechanism for policy deployment and impact.
- Multiple services that impact each other
- Change Management and new service coordination and communication
- 40 + Agency domains running in 1 tenant
- Policy and Sharing opportunities between Tenants
  - See Tenant Owner Guidance
- SLA understanding, negotiation and agreement
- Storage and licensing is pooled and not easily separated by Agency
Community of Practices (COP) Work Groups

- **O365 Governance**
  - Started 2\(^{nd}\) year

- **Email Administrators**
  - Kickoff 11/1 bi-monthly
  - COP SP Site

- **SharePoint**
  - Started Dec 2016
  - COP SP Site

- **Power BI Users Group**
  - Started August 2017
  - COP SP Site

- **Dynamics 365/CRM**
  - Starting November 2018

- **Desktop/Office Deployment**
  - Started 2\(^{nd}\) year / As needed
  - COP SP Site

- **O365 Tenant Owners**
  - Started in 2018
  - COP SP Site
<table>
<thead>
<tr>
<th>Responsibility</th>
<th>On-Prem</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data classification &amp; accountability</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client &amp; end-point protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity &amp; access management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application level controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[Cloud Customer: blue | Cloud Provider: gray]

Agency
Tenant Ownership

Microsoft
# Microsoft Responsibility

## Government Environments

- Store content in the continental United States
- Employ screened US citizens as Microsoft Admins

<table>
<thead>
<tr>
<th>Microsoft 365</th>
<th>Microsoft 365</th>
<th>Microsoft 365</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Government GCC</strong></td>
<td><strong>Government GCC High</strong></td>
<td><strong>Government DoD</strong></td>
</tr>
<tr>
<td>Best for FedRAMP Moderate impact data</td>
<td>Best for FedRAMP High impact data</td>
<td>Complies with DISA Level 5 Security Requirements Guidelines</td>
</tr>
<tr>
<td>Supports CJIS and IRS 1075</td>
<td>Supports ITAR and DFARS</td>
<td>For exclusive use by US Department of Defense</td>
</tr>
<tr>
<td>Complies with DISA Level 2 Security Requirements Guidelines</td>
<td>Complies with DISA Level 4 Security Requirements Guidelines</td>
<td></td>
</tr>
</tbody>
</table>


Microsoft Intelligent Security Graph

6.5 TRILLION signals per day

- 400B emails analyzed
- 1.2B devices scanned each month
- 200+ global cloud consumer and commercial services
- 18B+ Bing web pages scanned
- 450B monthly authentications
- 750M+ Azure user accounts
- 5B threats detected on devices every month

Shared threat data from partners, researchers, and law enforcement worldwide

Enterprise security for 90% of Fortune 500
Tenant Owner Responsibility =

- Manage Constant Change
- Lead COP Discussion
- Make Recommendations to Governance
- Build STRAC Service Package
- SMA Launch Service
- Assess New Services
- Research Management Controls
- Assess Security of the Service
Agency Responsibility =

Manage Constant Change
Agency Responsibility

• Stay up to date (OS, Hardware, Office updates)

• Endpoint Protection

• Data Classification

• Specific Service Decisions & Settings

• Send your Service admins/users to COP to learn what’s coming and security best practices

• Practice and Promote Governance and COP Recommendations
1 Year

2 Months

27 Days
<table>
<thead>
<tr>
<th></th>
<th>Windows XP</th>
<th>Windows Vista</th>
<th>Windows 7</th>
<th>Windows 8 / 8.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mainstream</td>
<td>14 April 2009</td>
<td>10 April 2012</td>
<td>13 January 2015</td>
<td>9 January 2018</td>
</tr>
<tr>
<td>support ends</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extended</td>
<td>8 April 2014</td>
<td>11 April 2017</td>
<td>14 January 2020</td>
<td>10 January 2023</td>
</tr>
<tr>
<td>support ends</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What is the Ideal State to consume O365 Services?
How many services do we offer in O365?

13 Active

7 Evaluating
Service Offerings

Available Offerings

- Dynamics 365
- Groups
- OneDrive for Business
- Email
- Intune MAM
- Planner
- Email Filtering/Relay
- Mailman
- Power BI
- Forms
- Office Graph/Delve
- SharePoint Online

Evaluating Offerings

- Cisco Collaboration Suite
- StaffHub
- Intune MDM
- Sway
- Microsoft Teams
- To Do
- PowerApps & Flow
What’s New?

- O365 Groups
- Intune MAM (Mobile Application Management)
- Power BI
O365 New Features
From MS Announcement to DIT Tenant Go Live

- Microsoft announces new service or feature
- 3 months Availability
  - First release for commercial
  - First release testing within test tenant

**Preview (Commercial)**

- 6 months Availability
  - To all commercial users
  - To all Test Tenant users

**General Availability (Commercial)**

- 6-12 months (FedRamp) Availability
  - First release users

**Preview (Government)**

- 3-6 months Availability
  - To all Government users

**General Availability (Government)**

- Turn off default service (if possible)
- Enable for COP testing (if possible)
- Develop Service Package
  - (R&R, Support Matrix, Security Controls, Management Controls, Onboarding Process and Policy)
- Develop and get STRAC Approved
Best Practices
Email Best Practices

- Use Encryption if Needed
- Use Rights Management
- DLP is set up for PII and PCI
- Implemented SPF, working on DKIM, DMARQ
- Removed Protocols not needed on every account. IMAP, SMTP, POP By default all were enabled.
- Piloting new email Security Gateway.
- Audit all MBX accounts.
- Train users Phishing Simulators
Email Encryption and DLP

Two ways you can trigger an encrypted email:

1. **Manually invoking encryption**
   Office Message Encryption – Manually send an encrypted email by typing [encrypt] in the subject line when you are working with external users. There must be space on either side of the bracket.

2. **Automatically triggering encryption**
   DLP (Data Loss Prevention) enforced Encryption - Automatic encryption based on set rules for sensitive data types (SSN/PII and PCI/Credit Card).

   Internal emails are automatically encrypted. TLS (Transport Layer Security) v 1.2 protocol for secure communication.
Most secure email gateway vendors are not responding fast enough to increasing levels of phishing attacks.

Security and risk managers (SRMs) should take a three-pronged approach to improving their defenses against phishing attacks:

1. Upgrade secure email gateway and other controls to improve protection for phishing.

2. Integrate employees into the solution and build capabilities to detect and respond to suspected attacks

3. Work with business managers to develop standard operating procedures for handling sensitive data and financial transactions.
Rights Management Emails

• Rights Management features:
  Do not forward, copy, print

• Some Rights Management Permissions only work for internal users. Ex. Confidential

• Encrypt & Do Not Forward work for External users.
Mobile Application Management (MAM) Best Practices

- Lock Down MS Applications on the phone.
- Set min OS level Android 6.0/iOS 8.1
- Block managed apps from running on jailbroken or rooted devices
- Set App PIN

- Select which storage services State data can be saved to OneDrive for Business & SharePoint
- Restrict cut, copy and paste with other apps.
- Encrypt data within scoped Apps
OneDrive/SharePoint Best Practices

- **Move to Modern Sites vs Classic SharePoint**
- **Use IRM for Sensitive Document Libraries**
  - Set up DLP
- **Lock down creation of sites and O365 Groups/Teams**
- **Block downloads for sensitive documents. Prevent users from downloading & copy and pasting documents.**
- **Sensitive data in Lists and Libraries should be excluded from Search/Delve**
  - Default is include in Search
- **Set document / Link expiration**
  - Default is 14 days
- **Only allow external sharing from specific sites and by Admins**
- **Set up a Private Folder in OneDrive**
- **Move to Office 2016 and Win 10 or use Browser.**
Security Controls to Protect Sensitive Data in SharePoint and OneDrive

• How to exclude items from SharePoint Search
• How to disable downloading of documents from SharePoint
• Working with Information Rights Management – Techniques/Tools
• MS Office Protections
• Working with Data Loss Prevention/Policies
Information Rights Management (IRM)

IRM helps protect sensitive files from being misused or distributed without permission once they have been downloaded from this library.

- Restrict permissions on this library on download
- Create a permission policy title
  - Add a permission policy description:

Set additional IRM library settings
This section provides additional settings that control the library behavior.

- Do not allow users to upload documents that do not support IRM
- Stop restricting access to the library at
  - 11/16/2018
- Prevent opening documents in the browser for this Document Library

Configure document access rights
This section control the document access rights (for viewers) after the document is downloaded from the library; read only viewing right is the default. Granting the rights below is reducing the bar for accessing the content by unauthorized users.

- Allow viewers to print
- Allow viewers to run script and screen reader to function on downloaded documents
- Allow viewers to write on a copy of the downloaded document
- After download, document access rights will expire after these number of days (1-365)
  - 90

Set group protection and credentials interval
Use the settings in this section to control the caching policy of the license the application that opens the document will use and to allow sharing the downloaded document with users that belong to a specified group.

- Users must verify their credentials using this interval (days)
  - 30
- Allow group protection. Default group:
  - Enter a name or email address...
DLP in SP and OD & How this works

- PII and PCI Customized Sensitive Data Templates enabled
- Monitoring and notifying. Not enforcing DLP policies yet.
- Send an incident report to the security liaison and notify the content owners with a Policy Tip if sensitive data is detected.
- Support for DLP and hits on Sensitive Data in Exchange, SharePoint and OneDrive need to be directed to the Agency Security Liaison.
- In order to see Policy Tips, Users need to use OWA or have 2013 or later Office ProPlus
Restore your OneDrive

If something went wrong, you can restore your OneDrive to a previous time. Select a date preset or use the slider to find a date with unusual activity in the chart. Then select the changes that you want to undo.

Select a date

Custom date and time

Restore  Cancel

Move the slider to quickly scroll the list to a day.
Coming Soon – Major Features

- **Planner**: Available on or around Oct 31st
- **Flow & PowerApps**: Available Q1 of 2019
- **Forms**: Available on or around Nov 1st

More info?
[https://ncconnect.sharepoint.com/sites/O365/SitePages/Home.aspx](https://ncconnect.sharepoint.com/sites/O365/SitePages/Home.aspx)
FUTURE APPROACH TO INFORMATION PROTECTION

Comprehensive protection of sensitive data throughout the lifecycle – inside and outside the organization

- **Detect**: Scan & detect sensitive data based on policy
- **Classify**: Classify data and apply labels based on sensitivity
- **Protect**: Apply protection actions, including encryption, access restrictions
- **Monitor**: Reporting, alerts, remediation

**Devices**

**Cloud**
Document labeling – what is it?

Metadata written into document files

Travels with the document as it moves

In clear text so that other systems such as a DLP engine can read it

Used for the purpose of apply a protection action or data governance action – determined by policy

Can be customized per the organization’s needs

More info?
Admin
- Creates a sensitivity label
- Publishes the sensitivity label to users and groups selected in a label policy

End user
- Works on an email or document and sees the available labels
- Classifies the document by applying a label

Office or third-party app/service
- Enforces protection settings on the email or document based on the applied label
Now...a boundary-less world
PROTECT SENSITIVE DATA ACROSS THE ENVIRONMENT

Cloud
- File encryption
- Secure External Sharing
- Permissions and rights-based restrictions
- DLP actions to prevent sharing
- Policy tips & notifications for end-users
- Visual markings in documents
- Control and protect data in cloud apps with granular policies and anomaly detection
- Data retention, expiration, deletion

Devices
- Drive encryption
- MAM/ Remote wipe
- MAM/ Business data separation
What’s Our Next Challenge?

Power Apps and Flow

- Built-in connectivity to 230+ SaaS cloud services, file providers, databases, web APIs, productivity apps, and more
- Connect to on-premises systems via Data Gateway
- Pluggable extensibility via Custom Connectors to integrate existing LOB systems into Flow
Nothing worse than a cloud-killer.
Cybersecurity is a **Shared** Responsibility!
Q & A
Contact your BRM or send an email to O365SME@nc.gov

Office 365 Service Packages, Training & Support

O365 Governance Site

Tenant Owners Site